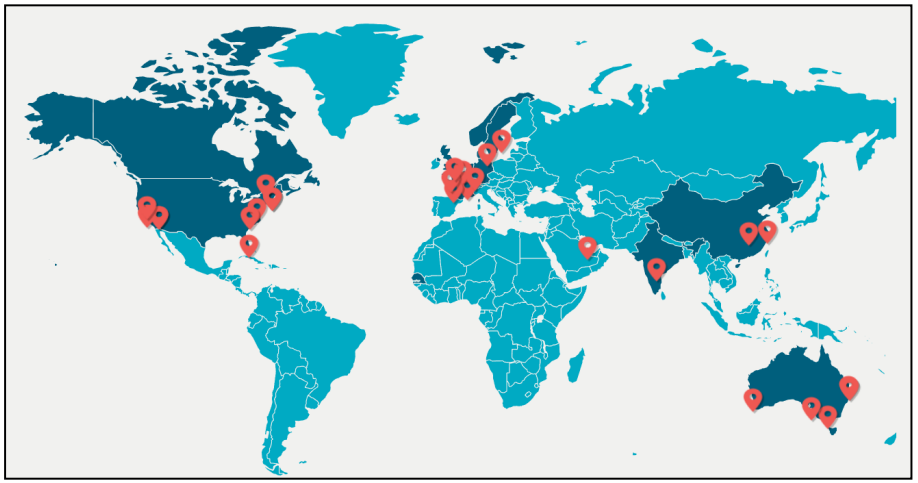
Filler Distro
Pittsburgh, PA
FillerPGH.wordpress.com

CRACKING SCREENS

A SCAM APP PRIMER

The website of the company that developed the ticketing software proudly showcases a map of the world marked with all of their customers in large metropolitan areas. In theory, the scam that was developed could have been reskinned to work on those transportation systems. If this one scam could work around the world, where else could we strike?



Further Reading

A Hacker Manifesto (Kenzie Work) ***https://monoskop.org/images/8/85/Wark_McKenzie_A_Hacker_Manifesto.pdf*** *theorizes emerging alliances, divisions and forms of conflict in information capitalism*

Postscript on the Societies of Control (Gilles Deleuze) ***https://theanarchistlibrary.org/library/gilles-deleuze-postscript-on-the-societies-of-control*** *conceptualizes a shift from disciplinary power to control and pushes us to create the new weapons we need*

The Exploit (Alexander Galloway, Eugene Thacker) ***http://dss-edit.com/plu/Galloway-Thacker_The_Exploit_2007.pdf*** *explores the new roles technology plays in control society & advocates for anonymous disruptive asymmetrical attacks*

Hacking: The Art of Exploitation (Jon Erickson) *a practical guide on how to identify vulnerabilities in programs... unfortunately it's hard to find online but it's usually pretty stealable at your local Barnes & Noble*

What is an Apparatus? (Giorgio Agamben) *an overview of how institutions and (social) technologies configure space and produce identities upon encountering living people*

Critical Metaphysics as a Science of Apparatuses (Tiqqun) ***https://archive.org/details/ill_will_2017_metaphysics*** *explores the implications of and offers practical suggestions for a criminal liquidation of all apparatuses*

To Our Friends (The Invisible Committee) ***https://theanarchistlibrary.org/library/the-invisible-committe-to-our-friends*** *don't miss the chapter Fuck Off, Google*

A Note About App Production: The train ticket app wasn't made by the train company, they contracted it out to a software development company. The companies offering "technical solutions" to shit that never needed an app in the first place will design dozens of apps and skin them for different customers.

Like most commodities in global capitalism, apps tend to be developed in a fragmented way; each stage of production will feature different workers, managers, companies. This presents a few considerations for any budding scammer. The employees you are interacting with likely have little to no technical knowledge about how the target app works, since chances are it was made by entirely different people in a cushy office hundreds of miles away.

The fragmentation inherent in the target app's production also meant that any sort of issue that the train company wanted to take with the scam could only be remedied by a coordinated series of bureaucratic exchanges with the software company – naturally this resulted in a lot of wasted time and money across the board.

There's probably a lot of low-hanging fruit out there just waiting to be scammed. Scam safely, scam hard, and be ready to have each other's back. Seriously, fuck their apps, fuck their smartworld, we all know how ridiculous this shit is. This was made with all the love in the world for those big hearted few who nurture the skills and sensibilities we need to stop participating in and perpetuating this bullshit.

Cracking Screens

A Scam App Primer

Smartphones are really fucking snitchy and nasty. From the exploitation needed to extract lithium, to the suicide-net factories where the phones are assembled, to the social othering of those who cannot afford them, to the anxious phantom-buzz in your pocket that teaches us to dread solitude... the world of the smartphone is tragically just beginning to gain momentum.

As crises erupt globally, nation-states will be racing to deploy the latest digital carceral infrastructure needed to predict and preemptively respond to "crime", manage populations, and regulate the movements of individuals. Meanwhile, many of us often find ourselves reliant on our phones to keep close with those far away, or to find the gigs that we need to work to gather resources – for a lot of us, phones are unfortunately a near-essential tool we rely on to move through the world.

I have no interest in arguing for some pure withdrawal from communications technology. Instead, I want to explore the ways that phone apps are produced in order to map out the exploits that can be found within them.

While we look for ways to mitigate the way technology mediates our lives, we also ought to find ways to hijack tech to get free shit and carry out new experiments in autonomy.

NEW COMMUNICATIONS TECHNOLOGY
=
NEW WAYS OF MAKING US TALK

Empire is everywhere nothing happens. In the past few years it's become impossible not to notice that all the boring social relations we've been forced into are being creepily reconfigured through some slick app or another. Engineers have always praised the emancipatory promises that technology allegedly carries with it in the form of automation, but it's obvious that most of what we are dealing with are data-mining surveillance apps that people use to purchase the time of some precarious worker. Every day, new apps are sloppily created so that we can go about getting food delivered or boarding public transportation. The social violence in this industry gentrifies cities, further marginalizing those ungrateful, unworthy residents who do not have a phone.

THE CONTROL SOCIETY IS A PARANOID SOCIETY

Apps are often rushed to the market, which means that they are usually developed with security as an afterthought. For example, many apps that are designed to streamline transactions operate with a single barcode that is not unique for each user, or even rely on employees to visually verify that the information on your screen is correct. *In these cases, it is easy to create a fake app that is indistinguishable from the real one with some beginner level programming and photoshop skills.*

This kind of scam was pulled off somewhat recently with an app used to buy train tickets between several large urban areas. Since this scam is no longer viable, it's a good example we can pick apart here to see how things work.

No matter what your desires are, these guidelines will help you understand how your scam will spread and minimize your chances of getting caught as the ball gets rolling:

- Always start slowly. As people begin to start using the scam, be extremely observant for any changes in employee behavior that could suggest that the spot has been blown. If you remember to start slowly, you can spread the word to pull the plug on scam before things get messy.

- Unless you take special precautions to limit who can use the scam, anyone who has it can distribute to more people whether or not you want them to.

- Your scam will only spread faster and farther as more people have access to it.

- **Never implicate yourself as the scam's creator.** If you want to send people links to the scam, use The Tor Browser to anonymously upload it online and share the link to *this cool thing you found* over secure channels.

If you want to retain some control over how people use the scam, you easily can program the app to crash after a given date. After that date, you have the option to redistribute the scam all over again with any new changes that might be needed. If you take this precaution and the scam stops working, people will have a limited amount of time to risk harm by continuing to use it.

If the idea of unleashing your scam during a moment of mass unrest interests is appealing, you need to keep the promotional material offline. Keep your scam low-key until the kettle is hot, and then hit the streets with guides on how to obtain the scam.

Testing

After creating a prototype of your scam and triple checking it against the actual app, it's time to take the leap and test it.

It's a good idea to not be doing anything else illegal while you are experimenting with the efficacy of your scam. Dress up in some nice scamofloge. Be sure to have a backup plan in case things go south: I make sure that I have enough money to perform the actual transaction in case things get derailed.

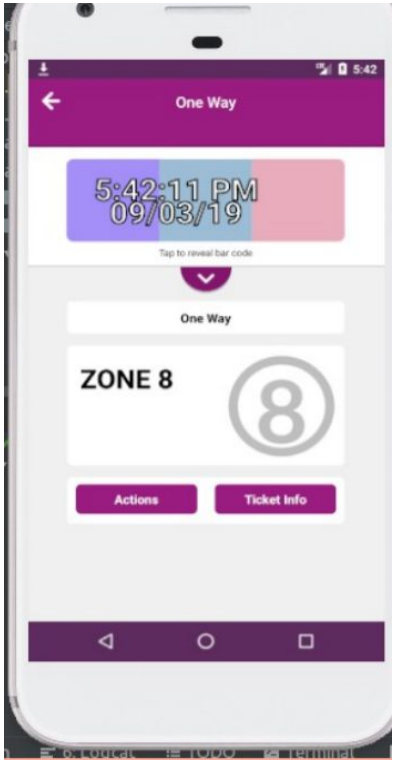
Social engineering is definitely a huge aspect, you should be confident in what you'll say and do to weasel out of sticky situations before you are stuck in one. If I'm ever in a pinch, I usually say that my phone is really old and apologize to the worker for wasting their time.

Distribution

Once you are confident that your scam works, you may consider distributing it. When a scam grows up and leaves the nest, it’s next to impossible to retain any control over who has it while remaining anonymous so you really should have some idea of how you want things to pan out beforehand.

Maybe you want your scam to be a tool kept within your circles so your friends can live that good life for a while, or maybe you’re more interested in a short and furious free fare party that pushes a *moment* further knowing that the free rides will end, but for a little while the party really begins.

The commercial train ticket app was essentially a fancy screen saver that displayed information about how much your ticket costs, along with an animation of the current date and time that scrolled across the screen. The transit system's overworked and underpaid conductors would visually verify that the information on your screen was correct. Instead of dropping that last $25, all you had to do was present them something that passed their inspection and you could ride for free whenever you wanted. From this simple realization, a scam was born.



In order to exploit oversights in an app, it is important to cultivate an understanding of how technology is being hastily used to "modernize" or "simplify" exchange.

If you understand how a scam could work, you can find the right people to make it *even if you do not posses the required skillset yourself.*

After working out the kinks, people boarded trains whenever they wanted to without paying. Free transportation quickly meant more free time – people worked less, found better work, or just ended up not working altogether due to better access to resources and like- minded people.

No longer merely a means to an end, transportation became a way for people to pursue leisure and joy in their lives. As the scam allowed people to move around freely, many began to view their environment in a radically different light.

Within weeks, the absurdity of the old fare situation became readily apparent: fatigued conductors hassling fatigued people for payments to get home, the aggressive deployment of security cameras across train stations, the chilling separation between alienated passengers sharing a seat. This misery, normally imperceptible or just taken for granted, became clearly recognized as something intolerable that was constructed to serve certain ends: the train company's scam.

If we are slaves of technology, this is precisely because there is a whole ensemble of artifacts of our everyday existence that we take to be specifically "technical" and that we will always regard simply as black boxes of which we are the innocent user.

[...] Understanding how the devices around us work brings an immediate increase in power, giving us a purchase on what will then no longer appear as an environment, but as a world arranged in a certain way and one that we can shape.

When our free fare scam was eventually shutdown, people didn't just forget about free transportation. Scams are a powerful way for people to imagine and work toward actualizing a more dignifying life.

People will never lose their love for free movement.

You Can Make a Scam App Too!

If you live in an urban environment, chances are there are similar opportunities out there for you.

First, identify your target. Once you have become familiar with how an app carries out a transaction you can start designing a scam app that mimics your target. For this, I prefer using Android smartphones because they are cheaper (even given out for free in some places), which makes for a more accessible hack.

Next, download the target app from the google play store and use the free development tools included in Android Studio. The free program apktool (https://ibotpeaches.github.io/Apktool/) can be used to decompile the target app which lets you see the application's code and graphical assets.

Often the decompiled code will be obfuscated, meaning you can't read it. However, the graphical assets will be useful and save you a lot of time when you are developing a scam application since you can just use the same assets rather than wasting time trying to create your own.

After looking for assets, install the target app into an Android emulator and walk through the transaction that you are trying to scam while capturing the networking traffic that the app uses to see if you can intercept information that's relevant to your attack.

You can use a free tool like Wireshark to observe all outgoing network requests through the Android emulator (https://stackoverflow.com/questions/2453949/android-emulator-how-to-monitor-network-traffic) Often you won't see anything useful because the target used SSL to encrypt their app's traffic, but you'd be surprised how often this isn't the case.